Speculo

SECURITY RISK ASSESSMENT

Service Definition Document

Service Overview

A security risk assessment is a systematic process used to identify, evaluate, and prioritise potential security risks and threats to an organisation's systems, networks, and data. It helps organisations understand their current security posture and make informed decisions to mitigate risks effectively.

Using the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework a globally recognised knowledge base of adversary tactics and techniques. This comprehensive catalogue of real-world cyber threats is used in this engagement to help organisations to assess their security risks alongside the controls against known attack tactics, techniques and procedures.

Service Scope

Scope Definition: A clearly defined scope of the assessment, including the systems, networks, and data assets to be evaluated. Identify the critical assets and potential threat vectors that need to be considered

Risk Identification: Analyse your systems, networks, and data assets to identify vulnerabilities and potential attack vectors. Use the MITRE ATT&CK framework to guide your analysis, focusing on tactics and techniques most relevant to your environment.

Threat Intelligence Gathering: Collect relevant threat intelligence from reputable sources, including MITRE ATT&CK, to understand the latest adversarial tactics and techniques. Stay updated on emerging threats and new attack vectors that might affect your organisation.

Risk Evaluation: Assess the impact and likelihood of each identified risk based on its potential to exploit vulnerabilities and cause harm to your organisation. Evaluate the potential business impact, including financial, reputational, and operational consequences. Prioritise risks based on their severity and likelihood of occurrence.

Framework Mapping: Map the relevant MITRE ATT&CK techniques to your organisation's security controls, including technologies, processes, and policies. This mapping helps identify any gaps or weaknesses in your defences and highlights areas requiring improvement.

Documentation and Reporting: Document the findings, assessments in a comprehensive report. Include actionable recommendations for improving security posture and provide clear insights to management and stakeholders about the organisation's risk landscape.

Benefits

Enhanced Security Posture: A security risk assessment helps organisations understand their current security posture. This knowledge allows them to implement appropriate controls and measures to mitigate risks effectively, thereby enhancing overall security posture**.**

Proactive Risk Management: By conducting a security risk assessment, organisations can identify and address potential risks before they are exploited by adversaries or cause significant damage. This proactive stance helps prevent security incidents and reduces the likelihood of costly breaches or disruptions.

Compliance and Regulatory Requirements: Many industries and jurisdictions have specific compliance and regulatory requirements for security. Conducting a security risk assessment helps organisations identify any gaps in compliance and ensure adherence to relevant regulations. It enables them to implement necessary controls and demonstrate due diligence in meeting compliance obligations.

Cost Savings: A security risk assessment helps organisations prioritise their security investments by identifying the most critical risks. By focusing resources on mitigating the highest-priority risks, organisations can optimise their spending and allocate funds where they are most needed. This approach can lead to cost savings by avoiding unnecessary expenditures on low-impact risks.

Incident Response Readiness: Understanding potential risks and vulnerabilities through a security risk assessment allows organisations the opportunity to develop robust incident

response plans. By anticipating potential threats and having predefined response procedures, organisations can start to plan to minimise the impact of incidents.

Stakeholder Confidence and Trust: A comprehensive security risk assessment demonstrates an organisation's commitment to protecting its assets and stakeholders' interests. It instils confidence in customers, partners, and shareholders by showcasing a proactive and well-managed security program.

Decision-making Support: A security risk assessment provides valuable insights and data that support informed decision-making at various levels within an organisation. It helps stakeholders understand the potential impact of security risks on business operations and helps the board to prioritise investments. This data-driven approach ensures that security decisions align with business objectives and risk appetite.

Continuous Improvement: A security risk assessment should not be a one-time exercise but an ongoing process. This promotes a culture of continuous improvement by regularly evaluating and updating security controls and strategies. By monitoring and reassessing risks over time, organisations can adapt their security posture to address emerging threats and maintain a strong defence against evolving attack techniques.